Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - ALZip Arbitrary Code Execution
  - BitDefender Anti-Virus Arbitrary Code Execution or Privilege Elevation
  - Citrix MetaFrame Security Restriction Bypassing
  - IceWarp Web Mail Cross Site Scripting or Directory Traversal
  - Macromedia Breeze Information Disclosure
  - MailEnable Arbitrary Code Execution
  - Merak Mail Server Arbitrary File Access
  - **Microsoft Jet Database Remote Code Execution Vulnerability (Updated)**
  - Microsoft Update Rollup 1 for Windows 2000 SP4
  - NateOn Messenger Arbitrary Code Execution or Denial of Service
  - **SecureW2 Information Disclosure (Updated)**
  - Symantec Anti Virus Arbitrary Code Execution
  - Virtools Web Player Arbitrary Code Execution or Arbitrary File Control
- UNIX / Linux Operating Systems
  - 4D WebStar Remote IMAP Denial of Service
  - **Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass (Updated)**
  - ApacheTop Insecure Temporary File Creation
  - **ClamAV UPX Buffer Overflow & FSG Handling Denial of Service (Updated)**
  - BackupNinja Insecure Temporary File Creation
  - **GNU CPIO CHMod File Permission Modification (Updated)**
  - **GNU CPIO Directory Traversal (Updated)**
  - **GNU Mailutils Format String (Updated)**
  - **GTKDiskFree Insecure Temporary File Creation (Updated)**
  - **HylaFAX Insecure Temporary File Creation (Updated)**
  - **IBM AIX Buffer Overflow (Updated)**
  - **Info-ZIP UnZip File Permission Modification (Updated)**
  - Mozilla Bugzilla Information Disclosure
  - **MPlayer Audio Header Buffer Overflow (Updated)**
  - Multiple Vendors Linux Kernel Coda_Pioctl Local Buffer Overflow
  - Multiple Vendors DIA Remote Arbitrary Code Execution
  - Multiple Vendors Cfengine Insecure Temporary Files
  - Multiple Vendors Linux Kernel Find_Target Local Denial of Service
  - **LBL TCPDump Remote Denials of Service (Updated)**
  - **Multiple Vendors RealNetworks RealPlayer & Helix Player Format String**
  - Multiple Vendors Squid NTLM Authentication Remote Denial of Service
  - **Multiple Vendors Linux Kernel XFRM Array Index Buffer Overflow (Updated)**
  - **Linux Kernel ZLib Null Pointer Dereference Denial of Service (Updated)**
  - **Zlib Compression Library Buffer Overflow (Updated)**
  - **Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service (Updated)**
  - Multiple Vendors Berkeley MPEG Tools Insecure Temporary File Creation
  - Multiple Vendors Gnome-PTY-Helper UTMP Hostname Spoofing
  - **Multiple Vendors Linux Kernel EXT2/EXT3 File Access Bypass (Updated)**
  - **Multiple Vendors Linux Kernel 'Ipt_recent' Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Buffer Overflow, Information Disclosure, & Denial of Service (Updated)**
  - Multiple Vendors OpenSSH LoginGraceTime Remote Denial of Service
  - **Linux Kernel ZLib Invalid Memory Access Denial of Service (Updated)**
  - **Multiple Vendors Util-Linux UMount Remounting Filesystem Elevated Privileges (Updated)**
  - **Multiple Vendors XFree86 Pixmap Allocation Buffer Overflow (Updated)**
  - **Net-SNMP Protocol Denial Of Service (Updated)**
  - NTLM Authorization Proxy Server Insecure Configuration File Permissions
  - **PCRE Regular Expression Heap Overflow (Updated)**
  - **ProFTPD Denial of Service or Information Disclosure (Updated)**
  - ProZilla Remote Buffer Overflow
  - SBLim-SFCB Malformed Header Denial of Service
  - **Squid Aborted Requests Remote Denial of Service (Updated)**
  - **Squid 'sslConnectTimeout()' Remote Denial of Service (Updated)**
  - StoreBackup Insecure Temporary File Creation

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
ALTools ALZip 5.52, 6.0, Korean 6.1	Multiple buffer overflow vulnerabilities have been reported in ALZip that could let remote malicious users execute arbitrary code. Upgrade to version 6.13: http://www.altools.net/ Currently we are not aware of any exploits for this vulnerability.	ALZip Arbitrary Code Execution	High	Security Focus, ID 15010, October 5, 2005

Bitdefender BitDefender AntiVirus 7.2, 8, 9	A vulnerability has been reported in BitDefender AntiVirus that could let remote malicious users execute arbitrary code or obtain elevated privileges. Upgrade to newest version via online upgrade tool. Currently we are not aware of any exploits for this vulnerability.	BitDefender Anti-Virus Arbitrary Code Execution or Privilege Elevation CAN-2005-3154	High	Secunia, Advisory: SA16991, October 4, 2005
Citrix MetaFrame Presentation Server 3.0, 4.0	A vulnerability has been reported in Citrix MetaFrame Presentation Server that could let remote malicious users to bypass security restrictions. Vendor workaround: http://support.citrix.com/kb/entry!default.jspa?categoryID=275&externalID=CTX107705 There is no exploit code required.	Citrix MetaFrame Security Restriction Bypassing CAN-2005-3134	Medium	SecurityTracker Alert ID: 1014994, September 30, 2005
Icewarp Web Mail 5.5.1	Multiple vulnerabilities have been reported in IceWarp Web Mail that could let remote malicious users conduct cross site scripting or traverse directories. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	IceWarp Web Mail Cross Site Scripting or Directory Traversal CAN-2005-3131 CAN-2005-3132 CAN-2005-3133	Medium	SecurityFocus, ID 14980, 14986, September 20, 2005
Macromedia Breeze 5.0	A vulnerability has been reported in the 'reset password' feature because passwords are stored in plaintext when the password is reset, which could let a malicious user obtain sensitive information. Updates available at: http://www.macromedia.com/support/breeze/licensed_support.html#item-2 There is no exploit code required.	Macromedia Breeze Information Disclosure CAN-2005-3112	Medium	Macromedia Security Bulletin MPSB 05-06, September 29, 2005
MailEnable Enterprise 1.1, Professional 1.6	A buffer overflow vulnerability has been reported in MailEnable that could let remote malicious users execute arbitrary code. Vendor hotfix available: http://www.mailenable.com/hotfix/ Currently we are not aware of any exploits for this vulnerability.	MailEnable Arbitrary Code Execution CAN-2005-3155	High	Secunia Advisory: SA17010, October 4, 2005
Merak Mail Server 8.2.4r	An input validation vulnerability has been reported in Merak Mail Server that could let remote malicious users access (delete) arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Merak Mail Server Arbitrary File Access CAN-2005-3133	Medium	SecurityFocus, ID 14988, September 30, 2005
Microsoft Jet Database msjet40.dll library version 4.00.8618.0	A vulnerability was reported that could let a remote malicious user cause arbitrary code to be executed. This is because the 'msjet40.dll' component does not properly validate user-supplied input when parsing database files. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Jet Database Remote Code Execution Vulnerability CAN-2005-0944	High	Hexview Advisory, ID: HEXVIEW*2005*03*31*1 **USCERT VU#176380, October 3, 2005**
Microsoft Update Rollup 1 for Windows 2000 SP4	Multiple vulnerabilities have been reported in various Microsoft products that could let malicious users perform a variety of functions. Apply Update Rollup: http://www.microsoft.com/downloads/details.aspx?amp;displaylang=en&familyid=B54730CF-8850-4531-B52B-BF28B324C662&displaylang=en	Microsoft Update Rollup 1 for Windows 2000 SP4 CAN-2005-3168 CAN-2005-3169 CAN-2005-3170 CAN-2005-3171 CAN-2005-3172 CAN-2005-3173 CAN-2005-3174 CAN-2005-3175 CAN-2005-3176 CAN-2005-3177	Medium	Microsoft Knowledge Base, ID 891861, September 28, 2005
NateOn Messenger	Multiple vulnerabilities have been reported in NateOn Messenger that could let remote malicious users cause a denial of service or execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	NateOn Messenger Arbitrary Code Execution or Denial of Service CAN-2005-3113 CAN-2005-3114	High	Secunia, Advisory: SA16983, October 4, 2005

SecureW2 3.0, 3.1.1	A vulnerability has been reported in SecureW2 that could let remote malicious users to disclose sensitive information. **Upgrade to version 3.1.2:** **http://www.securew2.com/uk/download/SecureW2_312.zip** Currently we are not aware of any exploits for this vulnerability.	SecureW2 Information Disclosure CAN-2005-3087	Medium	Secunia, Advisory: SA16909, September 26, 2005 SecurityFocus, ID 14947, October 3, 2005
Symantec Symantec AntiVirus Scan Engine 4.0, 4.3	A buffer overflow vulnerability has been reported in Symantec AntiVirus that could let remote malicious users execute arbitrary code. Vendor upgrade available: http://securityresponse.symantec.com/avcenter/security/Content/2005.10.04.html#savse4-3-12 Currently we are not aware of any exploits for this vulnerability.	Symantec Anti Virus Arbitrary Code Execution CAN-2005-2758	High	Symantec Security Response, SYM05-017, October 4, 2005
Virtools Web Player prior to 3.0.0.100	Multiple buffer overflow/ directory traversal vulnerabilities have been reported in Web Player that could let a remote malicious user execute arbitrary code or obtain arbitrary file control. Upgrade to version 3.0.0.101: http://player.virtools.com/downloads/playerie3.0.asp A Proof of Concept exploit script has been published.	Virtools Web Player Arbitrary Code Execution or Arbitrary File Control CAN-2005-3135 CAN-2005-3136	High	Secunia, Advisory: SA17034, October 3, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
4D Inc. WebSTAR 5.3-5.3.4, 5.2-5.2.4, 5.1.3, 5.1.2	A remote Denial of Service vulnerability has been report due to a failure to handle exceptional conditions. Upgrades available at: ftp://ftp.4d.com/products/webstar/current/4d_webstar_v/4DWSV_Security_535.sit There is no exploit code required.	4D WebStar Remote IMAP Denial of Service CAN-2005-3143	Low	Security Focus, Bugtraq ID: 14981, September 30, 2005
Apache Software Foundation Apache 2.0.x	A vulnerability has been reported in 'modules/ssl/ssl_engine_kernel.c' because the 'ssl_hook_Access()' function does not properly enforce the 'SSLVerifyClient require' directive in a per-location context if a virtual host is configured with the 'SSLVerifyCLient optional' directive, which could let a remote malicious user bypass security policies. Patch available at: http://svn.apache.org/viewcvs?rev=264800&view=rev OpenPKG: ftp://ftp.openpkg.org/release/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-608.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Debian: http://security.debian.org/pool/updates/main/	Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass CAN-2005-2700	Medium	Security Tracker Alert ID: 1014833, September 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.017, September 3, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 Ubuntu Security Notice, USN-177-1, September 07, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Debian Security Advisory, DSA 805-1, September 8, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:161, September 8, 2005 Slackware Security Advisory, SSA:2005-251-02, September 9, 2005 Trustix Secure Linux Security Advisory,

	a/apache2/ Mandriva: http://www.mandriva.com/security/advisories Slackware: ftp://ftp.slackware.com/pub/slackware/ Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/liba/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-12.xml Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-204.pdf **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required.			TSLSA-2005-0047, September 9, 2005 Debian Security Advisory DSA 807-1, September 12, 2005 US-CERT VU#744929 Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005 Avaya Security Advisory, ASA-2005-204, September 23, 2005 **Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005** **Turbolinux Security Advisory, TLSA-2005-94, October 3, 2005**
ApacheTop ApacheTop 0.12.5	A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user overwrite sensitive data. Debian: http://security.debian.org/pool/updates/main/a/apachetop/ There is no exploit code required.	ApacheTop Insecure Temporary File Creation CAN-2005-2660	Medium	Security Focus, Bugtraq ID: 14982, September 30, 2005 Debian Security Advisory, DSA 839-1, October 4, 2005
Clam Anti-Virus ClamAV 0.80 -0.86.2, 0.70, 0.65-0.68, 0.60, 0.51-0.54	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'libclamav/upx.c' due to a signedness error, which could let a malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported in 'libclamav/fsg.c' when handling a specially -crafted FSG-compressed executable file. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=86638 Gentoo: http://security.gentoo.org/glsa/glsa-200509-13.xml Mandriva: http://www.mandriva.com/security/advisories Trustix: http://http.trustix.org/pub/trustix/updates/ **Debian:** **http://security.debian.org/pool/updates/main/c/clamav/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for	ClamAV UPX Buffer Overflow & FSG Handling Denial of Service CAN-2005-2919 CAN-2005-2920	High	Secunia Advisory: SA16848, September 19, 2005 Gentoo Linux Security Advisory, GLSA 200509-13, September 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:166, September 20, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0051, September 23, 2005 **Debian Security Advisory DSA 824-1, September 29, 2005** **Conectiva Linux Announcement, CLSA-2005:1020, October 3, 2005**

	these vulnerabilities.			
Debian backupninja 0.5.2	A vulnerability has been reported in the 'backupninja' script due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges. Upgrade available at: http://security.debian.org/pool/updates/main/b/backupninja/backupninja_0.5-3sarge1_all.deb There is no exploit code required.	BackupNinja Insecure Temporary File Creation CAN-2005-3111	Medium	Debian Security Advisory, DSA 827-1, September 29, 2005
GNU cpio 1.0-1.3, 2.4.2, 2.5, 2.5.90, 2.6	A vulnerability has been reported when an archive is extracted into a world or group writeable directory because non-atomic procedures are used, which could let a malicious user modify file permissions. Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-378.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.32 Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-191.pdf Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cpio/** There is no exploit code required.	CPIO CHMod File Permission Modification CAN-2005-1111	Medium	Bugtraq, 395703, April 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA2005:116, July 12, 2005 RedHat Security Advisory, RHSA-2005:378-17, July 21, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 SCO Security Advisory, SCOSA-2005.32, August 18, 2005 Avaya Security Advisory, ASA-2005-191, September 6, 2005 Conectiva Linux Announcement, CLSA-2005:1002, September 13, 2005 **Ubuntu Security Notice, USN-189-1, September 29, 2005**
GNU cpio 2.6	A Directory Traversal vulnerability has been reported when invoking cpio on a malicious archive, which could let a remote malicious user obtain sensitive information. Gentoo: http://security.gentoo.org/glsa/glsa-200506-16.xml Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ Mandriva: http://www.mandriva.com/security/advisories SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.32 Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-191.pdf Conectiva: ftp://atualizacoes.conectiva.	CPIO Directory Traversal CAN-2005-1229	Medium	Bugtraq, 396429, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200506-16, June 20, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA2005:116, July 12, 2005 SCO Security Advisory, SCOSA-2005.32, August 18, 2005 Avaya Security Advisory, ASA-2005-191, September 6, 2005 Conectiva Linux Announcement, CLSA-2005:1002, September 13, 2005

	com.br/10/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/c/cpio/** A Proof of Concept exploit has been published.			**Ubuntu Security Notice, USN-189-1, September 29, 2005**
GNU Mailutils 0.6	A format string vulnerability has been reported in 'search.c' when processing user-supplied IMAP SEARCH commands, which could let a remote malicious user execute arbitrary code. Patch available at: http://savannah.gnu.org/patch/download.php?item_id=4407&item_file_id=5 160 Gentoo: http://security.gentoo.org/glsa/glsa-200509-10.xml **Debian:** **http://security.debian.org/pool/updates/main/m/mailutils/** An exploit script has been published.	GNU Mailutils Format String CAN-2005-2878	High	Security Tracker Alert ID: 1014879, September 9, 2005 Gentoo Linux Security Advisory, GLSA 200509-10, September 17, 2005 Security Focus, Bugtraq ID: 14794, September 26, 2005 **Debian Security Advisory, DSA 841-1, October 4, 2005**
GtkDiskFree GtkDiskFree 1.9.3	A vulnerability has been reported in the 'src/mount.c' file due to the insecure creation of temporary files, which could let a malicious user cause a Denial of Service or overwrite files. **Debian:** **http://security.debian.org/pool/updates/main/g/gtkdiskfree/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200510-01.xml** There is no exploit code required.	GTKDiskFree Insecure Temporary File Creation CAN-2005-2918	Medium	ZATAZ Audits Advisory, September 15, 2005 **Debian Security Advisory, DSA 822-1, September 29, 2005** **Gentoo Linux Security Advisory, GLSA 200510-01, October 3, 2005**
Hylafax Hylafax 4.2.1	Several vulnerabilities have been reported: a vulnerability was reported in the 'xferfaxstats' script due to the insecure creation of temporary files, which could let a remote malicious user create/overwrite arbitrary files; and a vulnerability was reported because ownership of the UNIX domain socket is not created or verified, which could let a malicious user obtain sensitive information and cause a Denial of Service. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-21.xml** There is no exploit code required.	HylaFAX Insecure Temporary File Creation CAN-2005-3069 CAN-2005-3070	Medium	Security Focus, Bugtraq ID: 14907, September 22, 2005 **Gentoo Linux Security Advisory, GLSA 200509-21, September 30, 2005**
IBM AIX 5.3 L, 5.3, 5.2.2, 5.2 L, 5.2	A buffer overflow vulnerability has been reported due to a failure to perform boundary checks prior to copying user-supplied data into insufficiently-sized memory buffers, which could let a malicious user execute arbitrary code. Update information available at: http://www-1.ibm.com/support/docview.wss?uid=isg1IY73850 http://www-1.ibm.com/support/docview.wss?uid=isg1IY73814 Currently we are not aware of any exploits for this vulnerability.	IBM AIX Buffer Overflow CAN-2005-3060	High	IBM Security Advisory, September 28, 2005 **US-CERT VU#602300**

Info-ZIP UnZip 5.52	A vulnerability has been reported due to a security weakness when extracting an archive to a world or group writeable directory, which could let a malicious user modify file permissions. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ SCO: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.39/507 **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/u/unzip/** **Trustix:** **http://http.trustix.org/pub/trustix/updates/** There is no exploit code required.	Info-ZIP UnZip File Permission Modification CAN-2005-2475	Medium	Security Focus, 14450, August 2, 2005 Fedora Update Notification, FEDORA-2005-844, September 9, 2005 SCO Security Advisory, SCOSA-2005.39, September 28, 2005 **Ubuntu Security Notice, USN-191-1, September 29, 2005** **Trustix Secure Linux Security Advisory, TSLSA-2005-0053, September 30, 2005**
Mozilla Bugzilla 2.18-2.21	Several vulnerabilities have been reported: a vulnerability was reported in the 'config.cgi' script because unauthorized access can be obtained even when the 'requirelogin' parameter is enabled, which could let a malicious user obtain sensitive information; and a vulnerability was reported in the user matching feature when the 'usevisibilitygroups' setting is enabled, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://ftp.mozilla.org/pub/mozilla.org/webtools/bugzilla-2.18.4.tar.gz There is no exploit code required.	Bugzilla Information Disclosure CAN-2005-3138 CAN-2005-3139	Medium	Bugzilla Security Advisory, September 30, 2005
MPlayer MPlayer 1.0 pre7, .0 pre6-r4, 1.0 pre6-3.3.5-20050130	A buffer overflow vulnerability has been reported due to insufficient validation of user-supplied strings, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200509-01.xml Mandriva: http://www.mandriva.com/security/advisories **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for this vulnerability.	MPlayer Audio Header Buffer Overflow CAN-2005-2718	High	Security Tracker Alert ID: 1014779, August 24, 2005 Gentoo Linux Security Advisory, GLSA 200509-01, September 1, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:158, September 7, 2005 **Conectiva Linux Announcement, CLSA-2005:1018, September 28, 2005**
Multiple Vendors Linux kernel 2.6-2.6.10, 2.4-2.4.28	A buffer overflow vulnerability has been reported in the 'coda_pioctl' function of the 'pioctl.c' file, which could let a malicious user cause a Denial of Service or execute arbitrary code with superuser privileges. RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Coda_Pioctl Local Buffer Overflow CAN-2005-0124	High	Security Focus, Bugtraq ID: 14967, September 28, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005
Multiple Vendors DIA 0.91-0.94; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A vulnerability has been reported in 'plug-ins/python/diasvg_import.py' due to the insecure use of the 'eval()' function when handling a malicious Scalable Vector Graphics (SVG) file, which could let a remote malicious user execute arbitrary python code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/d/dia/ A Proof of Concept exploit has been published.	DIA Remote Arbitrary Code Execution CAN-2005-2966	High	Security Focus, Bugtraq ID: 15000, October 3, 2005 Ubuntu Security Notice, USN-193-1, October 04, 2005

Multiple Vendors Cfengine 2.1.9, 2.1.8, 2.1.7 p1, 2.1 .0a9, 2.1.0a8, 2.1.0a6, 2.0.1-2.0.7 p1-p3, 2.0 .8p1, 2.0 .8, 2.0 .0, 1.6 a11, 1.6 a10, 1.5.3 -4, 1.5 x; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	Several vulnerabilities have been reported: a vulnerability was reported in '/bin/cfmailfilter' and '/contrib/cfcron.in' due to the insecure creation of temporary files, which could let a remote malicious user create/overwrite arbitrary files; and a vulnerability was reported in 'contrib/vicf.in/ due to the insecure creation of temporary files, which could let a remote malicious user create/overwrite arbitrary files. Debian: http://security.debian.org/pool/updates/main/c/cfengine/ There is no exploit code required.	Cfengine Insecure Temporary Files CAN-2005-2960	Medium	Debian Security Advisories, DSA 835-1 & 836-1, October 1, 2005
Multiple Vendors RedHat Enterprise Linux WS 3, ES 3, AS 3, Desktop 3.0; Linux kernel 2.4-2.4.28	A Denial of Service vulnerability has been reported in the 'find_target' function due to a failure to properly handle unexpected conditions when attempting to handle a NULL return value from another function. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.4/linux-2.4.29.tar.bz2 RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html There is no exploit code required.	Linux Kernel Find_Target Local Denial of Service CAN-2005-2553	Low	Security Focus, Bugtraq ID: 14965, September 28, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005

Multiple Vendors RedHat Fedora Core3; LBL tcpdump 3.9.1, 3.9, 3.8.1-3.8.3, 3.7-3.7.2, 3.6.3, 3.6.2, 3.5.2, 3.5, alpha, 3.4, 3.4 a6	A remote Denial of Service vulnerability has been reported in the 'bgp_update_print()' function in 'print-bgp.c' when a malicious user submits specially crafted BGP protocol data. Update available at: http://cvs.tcpdump.org/cgi-bin/cvsweb/tcpdump/print-bgp.c Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/tcpdump/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Slackware: ftp://ftp.slackware.com/pub/slackware IPCop: http://sourceforge.net/project/showfiles.php?group_id=40604&package_id=35093&release_id=351848 **IBM:** **http://www.ibm.com/support/** A Proof of Concept exploit script has been published.	TCPDump BGP Decoding Routines Denial of Service CAN-2005-1267	Low	Security Tracker Alert, 1014133, June 8, 2005 Fedora Update Notification, FEDORA-2005-406, June 9, 2005 Trustix Secure Linux Security Advisory, TLSA-2005-0028, June 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:101, June 15, 2005 Fedora Update Notification, FEDORA-2005-407, June 16, 2005 Ubuntu Security Notice, USN-141-1, June 21, 2005 Turbolinux Security Advisory, TLSA-2005-69, June 22, 2005 Slackware Security Advisory, SSA:2005-195-10, July 15, 2005 Security Focus, Bugtraq ID: 13906, August 26, 2005 **Security Focus, Bugtraq ID: 13906, October 3, 2005**
Multiple Vendors RedHat Fedora Core4, Core3, Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; Real Networks RealPlayer For Unix 10.0.4, 10.0.3, RealPlayer 10 for Linux , Japanese, German, English, Helix Player for Linux 1.0-1.0.4	A format string vulnerability has been reported when displaying an invalid-handle error message, which could let a remote malicious user execute arbitrary code. RedHat: http://rhn.redhat.com/errata/RHSA-2005-788.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Debian:** **http://security.debian.org/pool/updates/main/h/helix-player/** An exploit script has been published.	RealNetworks RealPlayer & Helix Player Format String CAN-2005-2710	High	RedHat Security Advisory, RHSA-2005:788-3, September 27, 2005 Fedora Update Notifications, FEDORA-2005-940 & 941, September 27, 2005 US-CERT VU#361181 **Debian Security Advisory DSA 826-1, September 29, 2005**
Multiple Vendors Squid Web Proxy Cache 2.5 .STABLE3-STABLE10, STABLE1	A remote Denial of Service vulnerability has been reported when handling certain client NTLM authentication request sequences.	Squid NTLM Authentication Remote Denial of	Low	Secunia Advisory: SA16992, September 30, 2005

	Upgrades available at: http://www.squid-cache.org/Versions/v2/2.5/squid-2.5.STABLE11.tar.gz Debian: http://security.debian.org/pool/updates/main/s/squid/ Currently we are not aware of any exploits for this vulnerability.	Service CAN-2005-2917		Debian Security Advisory, DSA 828-1, September 30, 2005
Multiple Vendors SuSE Linux Professional 9.3, x86_64, 9.2, x86_64, Linux Personal 9.3, x86_64; Linux kernel 2.6-2.6.12	A buffer overflow vulnerability has been reported in the XFRM network architecture code due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary code. Patches available at: http://www.kernel.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html **Mandriva: http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel XFRM Array Index Buffer Overflow CAN-2005-2456	High	Security Focus, 14477, August 5, 2005 Ubuntu Security Notice, USN-169-1, August 19, 2005 SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005**
Multiple Vendors Trustix Secure Linux 3.0, 2.2, Secure Enterprise Linux 2.0, SuSE Novell Linux Desktop 9.0, Linux Professional 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server for S/390 9.0, Linux Enterprise Server 9; 2.6-2.6.12 .4	A Denial of Service vulnerability has been reported due to a failure to handle malformed compressed files. Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.12.5.tar.gz Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ **Mandriva: http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ZLib Null Pointer Dereference Denial of Service CAN-2005-2459	Low	SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005**
Multiple Vendors zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64,	A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code. Debian: ftp://security.debian.org/pool/updates/main/z/zlib/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch Gentoo: http://security.gentoo.org/	Zlib Compression Library Buffer Overflow CAN-2005-2096	High	Debian Security Advisory DSA 740-1, July 6, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005 Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005 SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005 Ubuntu Security Notice,

ia-32, hppa, arm, alpha; zsync 0.4, 0.3-0.3.3, 0.2-0.2.3 , 0.1-0.1.6 1, 0.0.1-0.0.6	glsa/glsa-200507-05.xml SUSE: ftp://ftp.suse.com /pub/suse/ Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/z/zlib/ Mandriva: http://www.mandriva.com/ security/advisories OpenBSD: http://www.openbsd.org/ errata.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/ errata/RHSA-2005- 569.html Trustix: http://http.trustix.org/pub/ trustix/updates/ Slackware: ftp://ftp.slackware.com/ pub/slackware/ TurboLinux: ftp://ftp.turbolinux.co.jp/ pub/TurboLinux/ TurboLinux/ ia32/Server/10 Fedora: http://download.fedora. redhat.com/pub/fedora/ linux/core/updates/ zsync: http://prdownloads. sourceforge.net/zsync/ zsync-0.4.1.tar.gz? download Apple: http://docs.info.apple.com/ article.html?artnum= 302163 SCO: ftp://ftp.sco.com/pub/ updates/UnixWare/ SCOSA-2005.33 IPCop: http://sourceforge.net/ project/showfiles.php ?group_id=40604& package_id = 35093 &release_id=351848 Debian: http://security.debian.org/ pool/updates/main/ z/zsync/ Trolltech: ftp://ftp.trolltech.com/ qt/source/qt-x11-free- 3.3.5.tar.gz FedoraLegacy: http://download. fedoralegacy.org/ fedora/ Gentoo: http://security. gentoo.org/glsa/ glsa-200509-18.xml		USN-148-1, July 06, 2005 RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005 Fedora Update Notifications, FEDORA-2005-523, 524, July 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Slackware Security Advisory, SSA:2005-189-01, July 11, 2005 Turbolinux Security Advisory, TLSA-2005-77, July 11, 2005 Fedora Update Notification, FEDORA-2005-565, July 13, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Security Focus, 14162, July 21, 2005 USCERT Vulnerability Note VU#680620, July 22, 2005 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Security Focus, Bugtraq ID: 14162, August 26, 2005 Debian Security Advisory, DSA 797-1, September 1, 2005 Security Focus, Bugtraq ID: 14162, September 12, 2005 Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005 Gentoo Linux Security Advisory, GLSA 200509-18, September 26, 2005 **Gentoo Linux Security Advisory GLSA 200509-18, September 26, 2005**

	Gentoo: **http://security.gentoo.org/glsa/glsa-200509-18.xml** **Debian:** **http://security.debian.org/pool/updates/main/z/zsync/** Currently we are not aware of any exploits for this vulnerability.			**Debian Security Advisory, DSA 797-2, September 29, 2005**
Multiple Vendors zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input. Zlib: http://www.zlib.net/zlib-1.2.3.tar.gz Debian: http://security.debian.org/pool/updates/main/z/zlib/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ OpenBSD: http://www.openbsd.org/errata.html#libz2 Mandriva: http://www.mandriva.com/security/ advisories?name=MDKSA-2005:124 Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.323596 FreeBSD: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:18.zlib.asc SUSE: http://lists.suse.com/archive/suse-security-announce/2005-Jul/0007.html Gentoo: http://security.gentoo.org/glsa/glsa-200507-28.xml http://security.gentoo.org/glsa/glsa-200508-01.xml Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Apple: http://docs.info.apple.com/article.html?artnum=302163 TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/	Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service CAN-2005-1849	Low	Security Focus, Bugtraq ID 14340, July 21, 2005 Debian Security Advisory DSA 763-1, July 21, 2005 Ubuntu Security Notice, USN-151-1, July 21, 2005 OpenBSD, Release Errata 3.7, July 21, 2005 Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005 Secunia, Advisory: SA16195, July 25, 2005 Slackware Security Advisory, SSA:2005-203-03, July 22, 2005 FreeBSD Security Advisory, SA-05:18, July 27, 2005 SUSE Security Announcement, SUSE-SA:2005:043, July 28, 2005 Gentoo Linux Security Advisory, GLSA 200507-28, July 30, 2005 Gentoo Linux Security Advisory, GLSA 200508-01, August 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Conectiva Linux Announcement, CLSA-2005:997, August 11, 2005 Apple Security Update, APPLE-SA-2005-08-15, August 15, 2005 Turbolinux Security Advisory , TLSA-2005-83, August 18, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Debian Security Advisory, DSA 797-1, September 1, 2005 Security Focus, Bugtraq ID: 14340, September 12, 2005 Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005 **Debian Security**

	Server/10/updates/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33 Debian: http://security.debian.org/pool/updates/main/z/zsync/ Trolltech: ftp://ftp.trolltech.com/qt/source/qt-x11-free-3.3.5.tar.gz FedoraLegacy: http://download.fedoralegacy.org/fedora/ **Debian:** **http://security.debian.org/pool/updates/main/z/zsync/** Currently we are not aware of any exploits for this vulnerability.			**Advisory, DSA 797-2, September 29, 2005**
Multiple Vendors Gentoo Linux; Berkeley MPEG Tools Berkeley MPEG Tools 1.5 b	A vulnerability has been reported in MPEG tools due to the insecure creation of temporary files, which could let a malicious user overwrite sensitive data. Gentoo: http://security.gentoo.org/glsa/glsa-200510-02.xml There is no exploit code required.	Berkeley MPEG Tools Insecure Temporary File Creation CAN-2005-3115	Medium	Gentoo Linux Security Advisory, GLSA 200510-02, October 3, 2005
Multiple Vendors GNOME vte, ibzvt2 1.4.2; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A vulnerability has been reported in 'grone-pty-helper' due to insufficient validation of the 'DISPLAY' environment variable before recorded as the user's logon hostname, which could let a malicious user spoof the hostname information in UTMP. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Gnome-PTY-Helper UTMP Hostname Spoofing CAN-2005-0023	Medium	Security Focus, Bugtraq ID: 15004, October 3, 2005
Multiple Vendors Linux kernel 2.6.8, 2.6.10	A vulnerability has been reported in the EXT2/EXT3 file systems, which could let a remote malicious user bypass access controls. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel EXT2/EXT3 File Access Bypass CAN-2005-2801	Medium	Security Focus, Bugtraq ID: 14792, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005**
Multiple Vendors Linux kernel 2.6.8, 2.6.10	A remote Denial of Service vulnerability has been reported in the 'ipt_recent' module when specially crafted packets are sent. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'Ipt_recent' Remote Denial of Service CAN-2005-2872	Low	Security Focus, Bugtraq ID: 14791, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005**

Multiple Vendors Linux kernel 2.6.8-2.6.10, 2.4.21	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'msg_control' when copying 32 bit contents, which could let a malicious user obtain root privileges and execute arbitrary code; and a vulnerability was reported in the 'raw_sendmsg()' function, which could let a malicious user obtain sensitive information or cause a Denial of Service. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Buffer Overflow, Information Disclosure, & Denial of Service CAN-2005-2490 CAN-2005-2492	High	Secunia Advisory: SA16747, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Fedora Update Notifications, FEDORA-2005-905 & 906, September 22, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005**
Multiple Vendors RedHat Enterprise Linux WS 3, ES 3, AS 3, Desktop 3.0; OpenSSH 3.0-3.7.1, 2.9.9, 2.9 p1 & p2, 2.9, 2.5-2.5.2, 2.3	A remote Denial of Service vulnerability has been reported in the 'LoginGraceTime' server configuration device due to a design error when servicing timeouts. Upgrades available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/openssh-3.8.tgz There is no exploit code required.	OpenSSH LoginGraceTime Remote Denial of Service CAN-2004-2069	Low	Security Focus, Bugtraq ID: 14963, September 28, 2005 RedHat Security Advisory, RHSA-2005:550-6, September 28, 2005
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Trustix Secure Linux 3.0, 2.2, Trustix Secure Enterprise Linux 2.0; SuSE Novell Linux Desktop 9.0, Linux Professional 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server 9; Linux kernel 2.6-2.6.12 .4	A Denial of Service vulnerability has been reported due to a failure to handle exceptional conditions. Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.12.5.tar.gz Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ZLib Invalid Memory Access Denial of Service CAN-2005-2458	Low	SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005**
Multiple Vendors util-linux 2.8-2.13; Andries Brouwer util-linux 2.11 d, f, h, i, k, l, n, u, 2.10 s	A vulnerability has been reported because mounted filesystem options are improperly cleared due to a design flaw, which could let a remote malicious user obtain elevated privileges. Updates available at: http://www.kernel.org/pub/linux/utils/util-linux/testing/util-linux-2.12r-pre1.tar.gz Slackware: ftp://ftp.slackware.com/	Util-Linux UMount Remounting Filesystem Elevated Privileges CAN-2005-2876	Medium	Security Focus, Bugtraq ID: 14816, September 12, 2005 Slackware Security Advisory, SSA:2005-255-02, September 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005

	pub/slackware/ Trustix: http://http.trustix.org/ pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/ u/util-linux/ Gentoo: http://security.gentoo.org/ glsa/glsa-200509-15.xml Mandriva: http://www.mandriva.com/ security/advisories **Debian:** **http://security.debian.org/** **pool/updates/main/** **u/util-linux/** **SUSE:** **ftp://ftp.SUSE.com** **/pub/SUSE** There is no exploit code required.			Ubuntu Security Notice, USN-184-1, September 19, 2005 Gentoo Linux Security Advisory, GLSA 200509-15, September 20, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:167, September 20, 2005 **Debian Security Advisory, DSA 823-1, September 29, 2005** **SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005**
Multiple Vendors XFree86 X11R6 4.3 .0, 4.1 .0; X.org X11R6 6.8.2; RedHat Enterprise Linux WS 2.1, IA64, ES 2.1, IA64, AS 2.1, IA64, Advanced Workstation for the Itanium Processor 2.1, IA64; Gentoo Linux	A buffer overflow vulnerability has been reported in the pixmap processing code, which could let a malicious user execute arbitrary code and possibly obtain superuser privileges. Gentoo: http://security.gentoo.org/ glsa/glsa-200509-07.xml RedHat: http://rhn.redhat.com/ errata/RHSA- 2005-329.html http://rhn.redhat.com/ errata/RHSA- 2005-396.html Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/x/xfree86/ Mandriva: http://www.mandriva.com/ security/advisories?name =MDKSA-2005:164 Fedora: http://download.fedora. redhat.com/pub/ fedora/linux/ core/updates/ Trustix: http://http.trustix.org/ pub/trustix/updates/ Debian: http://security.debian.org/ pool/updates/main/ x/xfree86/ Sun: http://sunsolve.sun.com/ search/document.do? assetkey=1-26-101926-1 &searchclause SUSE: ftp://ftp.suse.com /pub/suse/ Slackware: ftp://ftp.slackware.com/ pub/slackware/ **Sun:** **http://sunsolve.sun.com/**	XFree86 Pixmap Allocation Buffer Overflow CAN-2005-2495	High	Gentoo Linux Security Advisory, GLSA 200509-07, September 12, 2005 RedHat Security Advisory, RHSA-2005:329-12 & RHSA-2005:396-9, September 12 & 13, 2005 Ubuntu Security Notice, USN-182-1, September 12, 2005 Mandriva Security Advisory, MDKSA-2005:164, September 13, 2005 US-CERT VU#102441 Fedora Update Notifications, FEDORA-2005-893 & 894, September 16, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Debian Security Advisory DSA 816-1, September 19, 2005 Sun(sm) Alert Notification Sun Alert ID: 101926, September 19, 2005 SUSE Security Announcement, SUSE-SA:2005:056, September 26, 2005 Slackware Security Advisory, SSA:2005-269-02, September 26, 2005 **Sun(sm) Alert Notification Sun Alert ID: 101953, October 3, 2005**

	search/document.do?assetkey=1-26-101953-1 Currently we are not aware of any exploits for this vulnerability.			
Net-SNMP Net-SNMP 5.2.1, 5.2, 5.1-5.1.2, 5.0.3 -5.0.9, 5.0.1	A remote Denial of Service vulnerability has been reported when handling stream-based protocols. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=12694&package_id=11571&release_id=338899 Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-720.html Mandriva: http://www.mandriva.com/security/advisories **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/net-snmp/** Currently we are not aware of any exploits for this vulnerability.	Net-SNMP Protocol Denial of Service CAN-2005-2177	Low	Secunia Advisory: SA15930, July 6, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Fedora Update Notifications, FEDORA-2005 -561 & 562, July 13, 2005 RedHat Security Advisory, RHSA-2005:720-04, August 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:137, August 11, 2005 **Ubuntu Security Notice, USN-190-1, September 29, 2005**
ntlmaps NTLM Authorization Proxy Server 0.9.9	A vulnerability has been reported in Authorization Proxy Server (ntlmaps) due to insecure permissions on the configuration file, which could let a malicious user obtain sensitive information. Debian: http://security.debian.org/pool/updates/main/n/ntlmaps/ There is no exploit code required.	NTLM Authorization Proxy Server Insecure Configuration File Permissions CAN-2005-2962	Medium	Debian Security Advisory, DSA 830-1, September 30, 2005

PCRE PCRE 6.1, 6.0, 5.0	A vulnerability has been reported in 'pcre_compile.c' due to an integer overflow, which could let a remote/local malicious user potentially execute arbitrary code. Updates available at: http://www.pcre.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/pcre3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-17.xml Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.SUSE.com/pub/SUSE Slackware: ftp://ftp.slackware.com/pub/slackware/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Debian: http://security.debian.org/pool/updates/main/p/pcre3/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-10.1/testing/packages/php-5.0.5/php-5.0.5-i486-1.tgz Gentoo: http://security.gentoo.org/glsa/glsa-200509-08.xml Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-12.xml Debian: http://security.debian.org/pool/updates/main/p/python2.2/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-19.xml Debian: http://security.debian.org/pool/updates/main/p/python2.3/ **Conectiva:**	PCRE Regular Expression Heap Overflow CAN-2005-2491	High	Secunia Advisory: SA16502, August 22, 2005 Ubuntu Security Notice, USN-173-1, August 23, 2005 Ubuntu Security Notices, USN-173-1 & 173-2, August 24, 2005 Fedora Update Notifications, FEDORA-2005-802 & 803, August 24, 2005 Gentoo Linux Security Advisory, GLSA 200508-17, August 25, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:151-155, August 25, 26, & 29, 2005 SUSE Security Announcements, SUSE-SA:2005:048 & 049, August 30, 2005 Slackware Security Advisories, SSA:2005-242-01 & 242-02 , August 31, 2005 Ubuntu Security Notices, USN-173-3, 173-4 August 30 & 31, 2005 Debian Security Advisory, DSA 800-1, September 2, 2005 SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005 Slackware Security Advisory, SSA:2005-251-04, September 9, 2005 Gentoo Linux Security Advisory, GLSA 200509-08, September 12, 2005 Conectiva Linux Announce-ment, CLSA-2005:1009, September 13, 2005 Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005 Debian Security Advisory, DSA 817-1 & DSA 819-1, September 22 & 23, 2005 Gentoo Linux Security Advisory, GLSA 200509-19, September 27, 2005 Debian Security Advisory, DSA 821-1, September 28, 2005 **Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005**

	ftp://atualizacoes.conectiva.com.br/10/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.			**Turbolinux Security Advisory, TLSA-2005-92, October 3, 2005**
ProFTPd	Multiple format string vulnerabilities have been reported in ProFTPd that could let remote malicious users cause a Denial of Service or disclose information. Upgrade to version 1.3.0rc2: http://www.proftpd.org/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200508-02.xml Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/p/proftpd/ OpenPKG: ftp://ftp.openpkg.org/release/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for these vulnerabilities.	ProFTPD Denial of Service or Information Disclosure CAN-2005-2390	Medium	Secunia, Advisory: SA16181, July 26, 2005 Gentoo Linux Security Advisory, GLSA 200508-02, August 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Turbolinux Security Advisory, TLSA-2005-82, August 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:140, August 16, 2005 Debian Security Advisories, DSA 795-1 & 795-2, September 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.020, September 6, 2005 **Conectiva Linux Announcement, CLSA-2005:1015, September 28, 2005**
Prozilla ProZilla Download Accelerator 1.3.0-1.3.7 .4, 1.0 x, 1.3.7.3	A buffer overflow vulnerability has been reported in 'ftpsearch.c' due to a boundary error when handling ftp search results in the 'get_string_ahref()' function, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/p/prozilla/ An exploit script has been published.	ProZilla Remote Buffer Overflow CAN-2005-2961	High	Debian Security Advisory, DSA 834-1, October 1, 2005
sblim sblim-sfcb 0.9.1, 0.9	A remote Denial of Service vulnerability has been reported due to a failure to handle malformed headers. Upgrades available at: http://prdownloads.sourceforge.net/sblim/sblim-sfcb-0.9.2.tar.bz2?down load There is no exploit code required.	SBLim-SFCB Malformed Header Denial of Service CAN-2005-3144 CAN-2005-3145	Low	Secunia Advisory: SA16975, September 29, 2005
Squid Web Proxy Squid Web Proxy Cache 2.5 & prior	A remote Denial of Service vulnerability has been reported in the 'storeBuffer()' function when handling aborted requests. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE10-STORE_PENDING.patch Gentoo:	Squid Aborted Requests Remote Denial of Service CAN-2005-2794	Low	Security Tracker Alert ID: 1014864, September 7, 2005 Gentoo Linux Security Advisory GLSA 200509-06, September 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.021, September 10, 2005

	http://security.gentoo.org/glsa/glsa-200509-06.xml OpenPKG: ftp://ftp.openpkg.org/release/ Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/s/squid/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/s/squid/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-766.html SUSE: ftp://ftp.suse.com/pub/suse/ **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** **Debian:** **http://security.debian.org/pool/updates/main/s/squid/** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.			Mandriva Linux Security Update Advisory, MDKSA-2005:162, September 12, 2004 Debian Security Advisory, DSA 809-1, September 13, 2005 Ubuntu Security Notice, USN-183-1, September 13, 2005 RedHat Security Advisory, RHSA-2005:766-7, September 15, 2005 SUSE Security Announcement, SUSE-SA:2005:053, September 16, 2005 **SGI Security Advisory, 20050903-02-U, September 28, 2005** **Conectiva Linux Announcement, CLSA-2005:1016, September 28, 2005** **Debian Security Advisory, DSA 809-2, September 30, 2005** **SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005** **Turbolinux Security Advisory, TLSA-2005-96, October 3, 2005**
Squid Web Proxy Squid Web Proxy Cache 2.5 .STABLE1-STABLE 10, 2.4 .STABLE6 & 7, STABLE 2, 2.4, 2.3 STABLE 4&5, 2.1 Patch 2, 2.0 Patch 2	A remote Denial of Service vulnerability has been reported in '/squid/src/ssl.c' when a malicious user triggers a segmentation fault in the 'sslConnectTimeout()' function. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE10-sslConnectTimeout.patch Trustix: http://http.trustix.org/pub/trustix/updates/ OpenPKG: ftp://ftp.openpkg.org/release/ Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ Debian: http://security.debian.org/pool/updates/main/s/squid/ RedHat:	Squid 'sslConnect Timeout()' Remote Denial of Service CAN-2005-2796	Low	Security Tracker Alert ID: 1014846, September 2, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.021, September 10, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:162, September 12, 2005 Ubuntu Security Notice, USN-183-1, September 13, 2005 Debian Security Advisory, DSA 809-1, September 13, 2005 RedHat Security Advisory, RHSA-2005:766-7, September 15, 2005 SUSE Security Announcement, SUSE-SA:2005:053,

	http://rhn.redhat.com/errata/RHSA-2005-766.html SUSE: ftp://ftp.suse.com/pub/suse/ **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.			September 16, 2005 **SGI Security Advisory, 20050903-02-U, September 28, 2005** **Conectiva Linux Announcement, CLSA-2005:1016, September 28, 2005** **SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005**
storeBackup storeBackup 1.18-1.18.4	A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user obtain sensitive information. Upgrades available at: http://prdownloads.sourceforge.net/storebackup/storeBackup-1.19.tar.bz 2?download SUSE: ftp://ftp.SUSE.com/pub/SUSE There is no exploit code required.	StoreBackup Insecure Temporary File Creation CAN-2005-3146 CAN-2005-3147 CAN-2005-3148	Medium	Security Focus, Bugtraq ID: 14985, September 30, 2005 SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005
Uim Uim 0.5 .0, 0.4.9	A vulnerability has been reported in 'uim/uim-custom.c' due to the incorrect use of several environment variables, which could let a malicious user obtain elevated privileges. Updates available at: http://uim.freedesktop.org/releases/uim-0.4.9.1.tar.gz There is no exploit code required.	Uim Elevated Privileges CAN-2005-3149	Medium	Secunia Advisory: SA17043, October 4, 2005
University of Minnesota gopherd 3.0.9	A buffer overflow vulnerability has been reported in the 'VlfromLine()' function when copying an input line, which could let a remote malicious user obtain unauthorized access. **Debian:** **http://security.debian.org/pool/updates/main/g/gopher/** An exploit script has been published.	UMN Gopher Client Remote Buffer Overflow CAN-2005-2772	Medium	Secunia Advisory: SA16614, August 30, 2005 US-CERT VU#619812 **Debian Security Advisory, DSA 832-1, September 30, 2005**
University of Washington UW-imapd imap-2004c1	A buffer overflow has been reported in UW-imapd that could let remote malicious users cause a denial of service or arbitrary code execution. Upgrade to version imap-2004g: ftp://ftp.cac.washington.edu/imap/ Currently we are not aware of any exploits for this vulnerability.	UW-imapd Denial of Service and Arbitrary Code Execution CAN-2005-2933	High	Secunia, Advisory: SA17062, October 5, 2005
Weex Weex 2.6.1 .5, 2.6.1	A format string vulnerability has been reported in the 'Log_Flush()' function when flushing an error log entry that contains format string specifiers, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Weex Format String CAN-2005-3150	High	Secunia Advisory: SA17028, October 3, 2005
Yukihiro Matsumoto Ruby 1.6 - 1.6.8, 1.8 - 1.8.2	A vulnerability has been reported in 'eval.c' due to a flaw in the logic that implements the SAFE level checks, which could let a remote malicious user bypass access restrictions to execute scripting code. Patches available at:	Ruby Safe Level Restrictions Bypass CAN-2005-2337	Medium	Security Tracker Alert ID: 1014948, September 21, 2005 **US-CERT VU#160012**

	ftp://ftp.ruby-lang.org/pub/ruby/1.6/1.6.8-patch1.gz Updates available at: http://www.ruby-lang.org/patches/ruby-1.8.2-xmlrpc-ipimethods-fix.diff There is no exploit code required.			
Yukihiro Matsumoto Ruby 1.8.2	A vulnerability has been reported in the XMLRPC server due to a failure to set a valid default value that prevents security protection using handlers, which could let a remote malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Debian: http://security.debian.org/pool/updates/main/r/ruby1.8/ Gentoo: http://security.gentoo.org/glsa/glsa-200507-10.xml Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-543.html Debian: http://security.debian.org/pool/updates/main/ Currently we are not aware of any exploits for this vulnerability.	Yukihiro Matsumoto Ruby XMLRPC Server Unspecified Command Execution CAN-2005-1992	High	Fedora Update Notifications, FEDORA-2005-474 & 475, June 21, 2005 Turbolinux Security Advisory, TLSA-2005-74, June 28, 2005 Debian Security Advisory, DSA 748-1, July 11, 2005 Gentoo Linux Security Advisory, GLSA 200507-10, July 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:118, July 13, 2005 RedHat Security Advisory, RHSA-2005:543-08, August 5, 2005 Debian Security Advisory, DSA 773-1, August 11, 2005 **US-CERT VU#684913**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Blender Blender 2.37 a	A buffer overflow vulnerability has been reported in 'blender' and 'blenderplay' due to a boundary error when handling command line inputs, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Blender Remote Buffer Overflow CAN-2005-3151	High	Security Focus, Bugtraq ID: 14983, September 30, 2005
Cube Cart CubeCart 3.0.3	Cross-Site Scripting vulnerabilities have been reported in the 'cart.php' and 'index.php' scripts due to insufficient filtering of HTML code from certain user-supplied input before displaying the input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at: http://www.cubecart.com/site/forums/index.php?act=Downloads There is no exploit code required; however, a Proof of Concept exploit script has been published.	CubeCart Multiple Cross-Site Scripting CAN-2005-3152	Medium	Security Tracker Alert ID: 1014984, September 28, 2005

Guppy EasyGuppy 4.5.5, 4.5.4	A Directory Traversal vulnerability has been reported in 'printfaq' due to insufficient sanitization, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.freeguppy.org/download.php?lng=en There is no exploit code required; however, a Proof of Concept exploit has been published.	EasyGuppy Directory Traversal CAN-2005-3156	Medium	Security Focus, Bugtraq ID: 14984, September 30, 2005
Hewlett Packard Company OpenView Network Node Manager 7.50 Solaris, 7.50, 6.41 Solaris, 6.41	A vulnerability has been reported in the 'node' URI parameter of the 'OvCgi/connected Nodes.ovpl' script, which could let a remote malicious user execute arbitrary code. Revision 3: Added PHSS_33783. Added preliminary files for OV NNM 7.01, 6.4, 6.2 Revision 4: Corrected files are available via ftp: README_HPSBMA01224_rev1.txt NNM6.2_HP-UX_CGI_Script_Point_Release_rev1.tar NNM6.2_HP-UX_CGI_Script_Point_Release_rev1.tar **Revision 5: Added PHSS_33842, PSOV_03430, and NNM_01110.** **Changed revision numbering (6.20, 6.4x instead of 6.2,6.4, 6.40, 6.41).** Workaround available at: http://support.openview.hp.com/news_archives.jsp There is no exploit code required; however, a Proof of Concept exploit script has been published.	HP OpenView Network Node Manager Remote Arbitrary Code Execution CAN-2005-2773	High	Portcullis Security Advisory, 05-014, August 25, 2005 HP Security Advisory, HPSBMA01224, August 26, 2005 HP Security Advisory, HPSBMA01224 REVISION: 3, September 13, 2005 HP Security Advisory, HPSBMA01224 REVISION: 4, September 19, 2005 **HP Security Advisory, HPSBMA01224 REVISION: 5, October 4, 2005**
Hitachi Hitachi Embedded Cosminexus Server Base 5.0, Embedded Cosminexus Server 5.0 , Cosminexus Primary Server Base 6.0, 5.0, Cosminexus Primary Server 6.0, Cosminexus Developer Standard 6.0, Cosminexus Developer Professional 6.0, Cosminexus Developer Light 6.0, Cosminexus Developer 5.0, Cosminexus Application Server Standard 6.0, Cosminexus Application Server Enterprise 6.0, Cosminexus Application Server 5.0	A vulnerability has been reported when a malformed HTTP post request is sent without a body, which could let a remote malicious user obtain sensitive information. Patches available at: http://www.hitachi-support.com/security_e/vuls_e/HS05-019_e/01-e.html There is no exploit code required.	Hitachi Cosminexus Remote Information Disclosure	Medium	Hitachi Security Advisory, HS05-019, September 30, 2005
Kaspersky Labs SMTP-Gateway for Linux/Unix 5.5, 5.0 , Antivirus for Linux Servers 5.5 -2, 5.0.1 .0, 3.5.135 .2, Antivirus 4.0.9.0, Antivirus Scanning Engine 5.0, 4.0, 3.0, Kaspersky Labs Anti-Virus 5.0.335, 5.0.228 , 5.0.227, Anti-Hacker 1.0	A heap overflow vulnerability has been reported during analysis of .CAB files, which could let a remote malicious user compromise the hosting computer. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Kaspersky Anti-Virus Library Remote Heap Overflow CAN-2005-3142	High	Security Focus, Bugtraq ID: 14998, October 3, 2005

lucidCMS lucidCMS 1.0 .11	An SQL injection vulnerability has been reported in login due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	lucidCMS Login SQL Injection CAN-2005-3130	Medium	Security Focus, Bugtraq ID: 14976, September 29, 2005
MediaWiki MediaWiki 1.4-1.4.8	Cross-Site Scripting vulnerabilities have been reported when handling '<math>' tags, extensions and '<nowiki>' sections due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/wikipedia/mediawiki-1.4.10.tar.gz?d ownload SUSE: ftp://ftp.SUSE.com/pub/SUSE There is no exploit code required.	MediaWiki Cross-Site Scripting CAN-2005-3165	Medium	Secunia Advisory: SA16932, September 30, 2005 SUSE Security Summary Report SUSE-SR:2005:021, September 30, 2005
Moritz Naumann SquirrelMail Address Add Plugin 2.0, 1.9	A Cross-Site Scripting vulnerability has been reported in 'add.php' due to insufficient sanitization of the 'first' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://squirrelmail.org/plugin_download.php?id=101&rev=1210 There is no exploit code required; however, a Proof of Concept exploit has been published.	SquirrelMail Cross-Site Scripting CAN-2005-3128	Medium	Security Tracker Alert ID: 1014988, September 29, 2005
Mozilla Firefox 1.0.6; Mozilla Browser 1.7.11, 1.7-1.7.9; Thunderbird 1.0-1.0.6	A vulnerability has been reported which could let a remote malicious user execute arbitrary commands via shell metacharacters in a URL. Upgrades available at: http://www.mozilla.org/products/firefox/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-785.html http://rhn.redhat.com/errata/RHSA-2005-789.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.479350 **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/**	Mozilla Browser/Firefox Arbitrary Command Execution CAN-2005-2968	High	Security Focus Bugtraq ID: 14888, September 21, 2005 Security Focus Bugtraq ID: 14888, September 22, 2005 RedHat Security Advisories, RHSA-2005:785-9 & 789-11, September 22, 2005 Ubuntu Security Notices, USN-USN-186-1 & 186-2, September 23 & 25, 2005 US-CERT VU#914681 Mandriva Linux Security Update Advisory, MDKSA-2005:169, September 26, 2005 Fedora Update Notifications, FEDORA-2005-926-934, September 26, 2005 Slackware Security Advisory, SSA:2005-269-01, September 26, 2005 **SGI Security Advisory, 20050903-02-U, September 28, 2005** **Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005** **Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005** **Turbolinux Security**

	TurboLinux: **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required; however, a Proof of Concept exploit has been published.			**Advisory, TLSA-2005-93, October 3, 2005**
Mozilla.org Firefox 0.x, 1.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error because untrusted events generated by web content are delivered to the browser user interface; a vulnerability was reported because scripts in XBL controls can be executed even when JavaScript has been disabled; a vulnerability was reported because remote malicious users can execute arbitrary code by tricking the user into using the 'Set As Wallpaper' context menu on an image URL that is really a javascript; a vulnerability was reported in the 'InstallTrigger.install()' function due to an error in the callback function, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error when handling 'data:' URL that originates from the sidebar, which could let a remote malicious user execute arbitrary code; an input validation vulnerability was reported in the 'InstallVersion.compareTo()' function when handling unexpected JavaScript objects, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because it is possible for remote malicious user to steal information and possibly execute arbitrary code by using standalone applications such as Flash and QuickTime to open a javascript: URL; a vulnerability was reported due to an error when handling DOM node names with different namespaces, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insecure cloning of base objects, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.mozilla.org/products/firefox/ Gentoo: ftp://security.gentoo.org/glsa/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/errata/RHSA-2005-586.html Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005& m=slackware-security.418880 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/epiphany-browser/ http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/ http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ SUSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/	Firefox Multiple Vulnerabilities CAN-2005-2260 CAN-2005-2261 CAN-2005-2262 CAN-2005-2263 CAN-2005-2264 CAN-2005-2265 CAN-2005-2267 CAN-2005-2269 CAN-2005-2270	High	Secunia Advisory: SA16043, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:120, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-14, July 15, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005 Fedora Update Notifications, FEDORA-2005-603 & 605, July 20, 2005 RedHat Security Advisory, RHSA-2005:586-11, July 21, 2005 Slackware Security Advisory, SSA:2005-203-01, July 22, 2005 US-CERT VU#652366 US-CERT VU#996798 Ubuntu Security Notices, USN-155-1 & 155-2 July 26 & 28, 2005 Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005 SUSE Security Announcement, SUSE-SA:2005:045, August 11, 2005 Debian Security Advisory, DSA 775-1, August 15, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Debian Security Advisory, DSA 777-1, August 17, 2005 Debian Security Advisory, DSA 779-1, August 20, 2005 Debian Security Advisory, DSA 781-1, August 23, 2005 Gentoo Linux Security Advisory, GLSA 200507-24, August 26, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:127-1, August 26, 2005 Slackware Security

	main/m /mozilla-firefox/ http://security.debian. org/pool/updates/ main/m/mozilla/ SGI: ftp://patches.sgi.com/ support/free/security/ advisories/ Gentoo: http://security.gentoo.org/ glsa/glsa-200507-24.xml Slackware: ftp://ftp.slackware.com/ pub/slackware/ Debian: http://security.debian. org/pool/updates/ main/m/ mozilla-firefox/ Debian: http://security.debian.org/ pool/updates/main/ m/mozilla/ Fedora: http://download.fedoralegacy. org/fedora/ HP: http://h20000.www2.hp.com/ bizsupport/TechSupport/ Document.jsp?objectID= PSD_HPSBOV01229 **HP:** **http://www.hp.com/ products1/unix/ java/mozilla/index.html** Exploits have been published.	Advisory, SSA:2005-085-01, August 28, 2005 Debian Security Advisory, DSA 779-2, September 1, 2005 Debian Security Advisory, DSA 810-1, September 13, 2005 Fedora Legacy Update Advisory, FLSA:160202, September 14, 2005 HP Security Bulletin, HPSBOV01229, September 19, 2005 **HP Security Bulletin, HPSBUX01230, October 3, 2005**

Mozilla.org Netscape 8.0.3.3, 7.2; Mozilla Firefox 1.5 Beta1, 1.0.6; Mozilla Browser 1.7.11; Mozilla Thunderbird 1.0.6	A buffer overflow vulnerability has been reported due to an error when handling IDN URLs that contain the 0xAD character in the domain name, which could let a remote malicious user execute arbitrary code. Patches available at: http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-769.html http://rhn.redhat.com/errata/RHSA-2005-768.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-11.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ **Gentoo: http://security.gentoo.org/glsa/glsa-200509-11.xml** **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/** **TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** A Proof of Concept exploit script has been published.	Mozilla/Netscape/ Firefox Browsers Domain Name Buffer Overflow CAN-2005-2871	High	Security Focus, Bugtraq ID: 14784, September 10, 2005 RedHat Security Advisories, 769-8 & RHSA-2005:768-6, September 9, 2005 Fedora Update Notifications, FEDORA-2005-871-184, September 10, 2005 Ubuntu Security Notice, USN-181-1, September 12, 2005 US-CERT VU#573857 Gentoo Linux Security Advisory GLSA 200509-11, September 18, 2005 Security Focus, Bugtraq ID: 14784, September 22, 2005 Slackware Security Advisory, SSA:2005-269-01, September 26, 2005 **Gentoo Linux Security Advisory [UPDATE], GLSA 200509-11:02, September 29, 2005** **Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005** **Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005** **Debian Security Advisory, DSA 837-1, October 2, 2005** **Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005**
Multiple Vendors Mozilla Firefox 1.0-1.0.6; Mozilla Browser 1.7-1.7.11	Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when processing malformed XBM images, which could let a remote malicious user execute arbitrary code; a vulnerability has been reported when unicode sequences contain 'zero-width non-joiner' characters, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability was reported due to a flaw when making XMLHttp requests, which could let a remote malicious user spoof XMLHttpRequest headers; a vulnerability was reported because a remote malicious user can create specially crafted HTML that spoofs XML objects to create an XBL binding to execute arbitrary JavaScript with elevated (chrome) permissions; an integer overflow vulnerability was reported in the JavaScript engine, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported because a remote malicious user can load privileged 'chrome' pages from an unprivileged 'about:' page, which could lead to unauthorized access; and a window spoofing vulnerability has been reported when a blank 'chrom' canvas is obtained by opening a window from a reference to a closed window, which could let a remote malicious user conduct phishing type attacks. Firefox: http://www.mozilla.org/	Mozilla Browser / Firefox Multiple Vulnerabilities CAN-2005-2701 CAN-2005-2702 CAN-2005-2703 CAN-2005-2704 CAN-2005-2705 CAN-2005-2706 CAN-2005-2707	High	Mozilla Foundation Security Advisory, 2005-58, September 22, 2005 RedHat Security Advisory, RHSA-2005:789-11, September 22, 2005 Ubuntu Security Notices, USN-186-1 & 186-2, September 23 & 25, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:169 & 170, September 26, 2005 Fedora Update Notifications, FEDORA-2005-926-934, September 26, 2005 Slackware Security

	products/firefox/ Mozilla Browser: http://www.mozilla.org/products/mozilla1.x/ RedHat: https://rhn.redhat.com/errata/RHSA-2005-789.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.479350 **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-11.xml** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Debian:** **http://security.debian.org/pool/updates/main/m/mozilla-firefox/** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.			Advisory, SSA:2005-269-01, September 26, 2005 **SGI Security Advisory, 20050903-02-U, September 28, 2005** **Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005** **Gentoo Linux Security Advisory [UPDATE] , September 29, 2005** **SUSE Security Announcement, SUSE-SA:2005:058, September 30, 2005** **Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005** **Debian Security Advisory, DSA 838-1, October 2, 2005** **Turbolinux Security Advisory ,TLSA-2005-93, October 3, 2005**
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; AbiSource Community AbiWord 2.2 .0-2.2.9, 2.0.1-2.0.9	A buffer overflow vulnerability has been reported in the RTF importer due to a boundary error, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.abisource.com/downloads/abiword/2.2.10/source/abiword-2.2.1 0.tar.gz Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/abiword/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-20.xml	AbiWord RTF File Processing Remote Buffer Overflow CAN-2005-2964	High	Security Tracker Alert ID: 1014982, September 28, 2005 Ubuntu Security Notice, USN-188-1, September 29, 2005 Fedora Update Notification, FEDORA-2005-955, September 30, 2005 Gentoo Linux Security Advisory, GLSA 200509-20, September 30, 2005

	Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Gentoo Linux; Apache Software Foundation Apache 2.1-2.1.5, 2.0.35-2.0.54, 2.0.32, 2.0.28, Beta, 2.0 a9, 2.0	A remote Denial of Service vulnerability has been reported in the HTTP 'Range' header due to an error in the byte-range filter. Patches available at: http://issues.apache.org/bugzilla/attachment.cgi?id=16102 Gentoo: http://security.gentoo.org/glsa/glsa-200508-15.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-608.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Debian: http://security.debian.org/pool/updates/main/a/apache2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.SUSE.com/pub/SUSE Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-204.pdf **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** **TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required.	Apache Remote Denial of Service CAN-2005-2728	Low	Secunia Advisory: SA16559, August 25, 2005 Security Advisory, GLSA 200508-15, August 25, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 Ubuntu Security Notice, USN-177-1, September 07, 2005 Fedora Update Notifications, FEDORA-2005-848 & 849, September 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:161, September 8, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Debian Security Advisory, DSA 805-1, September 8, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005 SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005 Avaya Security Advisory, ASA-2005-204, September 23, 2005 **Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005** **Turbolinux Security Advisory, TLSA-2005-94, October 3, 2005**
Multiple Vendors PHPXMLRPC 1.1.1; PEAR XML_RPC 1.3.3; Drupal 4.6-4.6.2, 4.5- 4.5.4; Nucleus CMS Nucleus CMS 3.21, 3.2, 3.1, 3.0, RC, 3.0.; MailWatch for MailScanner 1.0.1; eGroupWare 1.0.6, 1.0.3, 1.0.1, 1.0.0.007, 1.0	A vulnerability has been reported in XML-RPC due to insufficient sanitization of certain XML tags that are nested in parsed documents being used in an 'eval()' call, which could let a remote malicious user execute arbitrary PHP code. PHPXMLRPC : http://prdownloads.sourceforge.net/phpxmlrpc/xmlrpc.1.2.tgz?download Pear: http://pear.php.net/get/XML_RPC-1.4.0.tgz Drupal: http://drupal.org/files/projects/drupal-4.5.5.tar.gz eGroupWare:	PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution CAN-2005-2498	High	Security Focus, Bugtraq ID 14560, August 15, 2995 Security Focus, Bugtraq ID 14560, August 18, 2995 RedHat Security Advisory, RHSA-2005:748-05, August 19, 2005 Ubuntu Security Notice, USN-171-1, August 20, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:146,

http://prdownloads.sourceforge.net/egroupware/eGroupWare-1.0.0.009.tar .gz?download

MailWatch:
http://prdownloads.sourceforge.net/mailwatch/mailwatch-1.0.2.tar.gz

Nucleus:
http://prdownloads.sourceforge.net/nucleuscms/nucleus-xmlrpc-patch.zip ?download

RedHat:
http://rhn.redhat.com/errata/RHSA-2005-748.html

Ubuntu:
http://security.ubuntu.com/ubuntu/pool/main/p/php4/

Mandriva:
http://www.mandriva.com/security/advisories

Gentoo:
http://security.gentoo.org/glsa/glsa-200508-13.xml

http://security.gentoo.org/glsa/glsa-200508-14.xml

http://security.gentoo.org/glsa/glsa-200508-18.xml

Fedora:
http://download.fedora.redhat.com/pub/fedora/linux/core/updates/

Debian:
http://security.debian.org/pool/updates/main/p/php4/

SUSE:
ftp://ftp.suse.com/pub/suse/

Gentoo:
http://security.gentoo.org/glsa/glsa-200508-20.xml

http://security.gentoo.org/glsa/glsa-200508-21.xml

Slackware:
ftp://ftp.slackware.com/pub/slackware/

Debian:
http://security.debian.org/pool/updates/main/p/phpgroupware/

SGI:
ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/

Slackware:
ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/

ftp://ftp.slackware.com/

August 22, 2005

Gentoo Linux Security Advisory, GLSA 200508-13 & 14, & 200508-18, August 24 & 26, 2005

Fedora Update Notifications, FEDORA-2005-809 & 810, August 25, 2005

Debian Security Advisory, DSA 789-1, August 29, 2005

SUSE Security Announcement, SUSE-SA:2005:049, August 30, 2005

Gentoo Linux Security Advisory, GLSA GLSA 200508-20& 200508-21, August 30 & 31, 2005

Slackware Security Advisory, SSA:2005-242-02, August 31, 2005

Debian Security Advisory, DSA 798-1, September 2, 2005

SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005

SGI Security Advisory, 20050901-01-U, September 7, 2005

Slackware Security Advisories, SSA:2005-251-03 & 251-04, September 9, 2005

Gentoo Linux Security Advisory, GLSA 200509-19, September 27, 2005

Debian Security Advisory, DSA 840-1, October 4, 2005

	pub/slackware/ slackware-10.1/ testing/packages/ php-5.0.5/php-5.0.5 -i486-1.tgz Gentoo: http://security.gentoo.org/ glsa/glsa-200509-19.xml **Debian:** **http://security.debian.org/** **pool/updates/main/** **d/drupal/** There is no exploit code required.			
MySQL AB MySQL 5.0 .0-0-5.0.4, 4.1 .0-0-4.1.5, 4.0.24, 4.0.21, 4.0.20 , 4.0.18, 4.0 .0-4.0.15	A buffer overflow vulnerability has been reported due to insufficient bounds checking of data that is supplied as an argument in a user-defined function, which could let a remote malicious user execute arbitrary code. This issue is reportedly addressed in MySQL versions 4.0.25, 4.1.13, and 5.0.7-beta available at: http://dev.mysql.com /downloads/ Mandriva: http://www.mandriva.com/ security/advisories Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/ m/mysql-dfsg **Debian:** **http://security.debian.org/** **pool/updates/main/m/** **SUSE:** **ftp://ftp.SUSE.com** **/pub/SUSE** **Debian:** **http://security.debian.org/** **pool/updates/main/** **m/mysql-dfsg-4.1/** Currently we are not aware of any exploits for this vulnerability.	MySQL User-Defined Function Buffer Overflow CAN-2005-2558	High	Security Focus 14509 , August 8, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:163, September 12, 2005 Ubuntu Security Notice, USN-180-1, September 12, 2005 **Debian Security Advisories, DSA 829-1 & 831-1, September 30, 2005** **SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005** **Debian Security Advisory, DSA 833-1, October 1, 2005**
myWebland MyBloggie 2.1.3 beta	An SQL injection vulnerability has been reported in the 'login.php' script due to insufficient validation of the 'username' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	MyBloggie SQL Injection CAN-2005-3153	Medium	Security Tracker Alert ID: 1014995, October 3, 2005
PHP-Fusion PHP-Fusion 6.0.109	SQL injection vulnerabilities have been reported in 'photogallery.php' due to insufficient sanitization of the 'album' and 'photo' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	PHP-Fusion Multiple SQL Injection CAN-2005-3157	Medium	Secunia Advisory: SA17048, October 4, 2005
PHP-Fusion PHP-Fusion 6.0.109	An SQL injection vulnerability has been reported in 'messages.php' due to insufficient sanitization of the 'msg_send' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHP-Fusion SQL Injection	Medium	Secunia Advisory: SA16994, September 29, 2005
Polipo Polipo 0.9-0.9.8	A vulnerability has been reported because files can be exposed outside of the local root, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.pps.jussieu.fr/ ~jch/software/files/polipo/ polipo-0.9.9.tar. gz Currently we are not aware of any exploits for this vulnerability.	Polipo Web Root Restriction Bypass CAN-2005-3163	Medium	Security Focus, Bugtraq ID: 14970, September 28, 2005

Real Networks RealPlayer G2, 6.0 Win32, 6.0, 7.0 Win32, 7.0 Unix, 7.0 Mac, 8.0 Win32, 8.0 Unix, 8.0 Mac, 10.0 BETA, 10.0 v6.0.12.690, 10.0, 0.5 v6.0.12.1059 10.5 v6.0.12.1056, v6.0.12.1053, v6.0.12.1040, 10.5 Beta v6.0.12.1016, 10.5, 10 Japanese, German, English, 10 for Linux, 10 for Mac OS Beta, 10 for Mac OS 10.0.0.325, 10 for Mac OS 10.0.0.305, 10 for Mac OS, 10 for Mac OS 10.0 v10.0.0.331, RealPlayer 8, RealPlayer Enterprise 1.1, 1.2, 1.5-1.7, RealPlayer For Unix 10.0.3, 10.0.4, RealPlayer for Windows 7.0, RealPlayer Intranet 7.0, 8.0	A vulnerability has been reported when a specially crafted media file is opened, which could let a remote malicious user execute arbitrary code. RealNetworks: http://service.real.com/help/faq/security/050623_player/EN/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-517.html http://rhn.redhat.com/errata/RHSA-2005-523.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Gentoo: http://security.gentoo.org/glsa/glsa-200507-04.xml **Debian:** **http://security.debian.org/pool/updates/main/h/helix-player/** Currently we are not aware of any exploits for this vulnerability.	RealNetworks RealPlayer Unspecified Code Execution CAN-2005-1766	High	eEye Digital Security Advisory, EEYEB-20050504, May 5, 2005 RedHat Security Advisories, RHSA-2005:517-02 & RHSA-2005:523-05, June 23, 2005 Fedora Update Notifications, FEDORA-2005-483 & 484, June 25, 2006 SUSE Security Announce-ment, SUSE-SA:2005:037, June 27, 2005 Gentoo Linux Security Advisory, GLSA 200507-04, July 6, 2005 **Debian Security Advisory, DSA 826-1, September 30, 2005**
Sun Microsystems, Inc. OpenOffice 1.1.4, 2.0 Beta	A vulnerability has been reported due to a heap overflow when a specially crafted malformed '.doc' file is opened, which could lead to a Denial of Service or execution of arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-13.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-375.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/o/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	OpenOffice Malformed Document Remote Heap Overflow CAN-2005-0941	High	Security Focus, 13092, April 11, 2005 Fedora Update Notification, FEDORA-2005-316, April 13, 2005 Gentoo Linux Security Advisory, GLSA 200504-13, April 15, 2005 SUSE Security Announcement, SUSE-SA:2005:025, April 19, 2005 RedHat Security Advisory, RHSA-2005:375-07, April 25, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:082, May 6, 2005 Ubuntu Security Notice, USN-121-1, May 06, 2005 **SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005**

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **10 ways to wireless security:** Wireless networking is easy to set up and convenient but more vulnerable to interception and attack than a wired connection. Ten

tips for securing wireless can be found at: http://insight.zdnet.co.uk/communications/wireless/0,39020430,39223889,00.htm.

Wireless Vulnerabilities

- Nothing significant to report.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
October 4, 2005	ciscocrack2.c	N/A	Updated version of ciscocrack.c that works with newer versions of IOS.
October 4, 2005	Fusionv-6.00.109.txt	No	Exploit for the PHP-Fusion information disclosure vulnerability.
October 4, 2005	fr-dyn0.txt	N/A	A cross site scripting exploit for friendsreunited.co.uk lost password functionality.
October 4, 2005	lucid_cms_1011_expl.txt	No	Exploit for the Lucid CMS SQL Injection, Login Bypass, and remote code execution vulnerabilities.
October 4, 2005	mybloggie213b.txt	No	Script that exploits the MyBloggie SQL Injection vulnerability.
October 4, 2005	virtbugs.c virtools.3.0.0.100.txt	Yes	Exploits for the Virtools Web Player Buffer Overflow and Directory Traversal vulnerabilities.
October 3, 2005	gnome_pty_helper.c	No	Proof of Concept exploit for the Gnome-PTY-Helper UTMP Hostname Spoofing vulnerability.
September 30, 2005	prozilla.c	Yes	Script that exploits the ProZilla Remote Buffer Overflow vulnerability.
September 29, 2005	cubecart-3.0.3.txt	Yes	Exploitation for the CubeCart Multiple Cross-Site Scripting vulnerabilities.
September 29, 2005	mantis-poc.tar.gz	N/A	Mantis Bugtracker exploit scanner that looks for versions less than 1.0.0RC2 and greater than 0.18.3 which are vulnerable to XSS and variable poisoning attacks if register_globals is enabled.
September 28, 2005	PhpF6_00_109xpl.php phpfusion600109.txt Fusionv-6.00.109.txt	No	Proof of Concept exploits for the PHP-Fusion SQL Injection vulnerability.
September 28, 2005	zabypass.zip	No	Proof of Concept exploit for the Zone Labs ZoneAlarm Pro DDE-IPC Advanced Program Control Bypass vulnerability.

[back to top]

Trends

- **Microsoft's five-month Office flaw exploited:** Security experts are warning that a new Trojan horse exploits an unpatched flaw in Microsoft Office and could let an attacker take control of vulnerable computers. According to Symantec in an advisory they released, the Trojan horse arrives in the guise of a Microsoft Access file. The malicious code takes advantage of a flaw in Microsoft's Jet Database Engine. The security hole was reported to Microsoft in April but the company has yet to provide a fix for the problem. "Microsoft is aware that a Trojan recently released into the wild may be exploiting a publicly reported vulnerability in Microsoft Office." The software maker is investigating the issue and will take "appropriate action", the representative said. Source: http://software.silicon.com/malware/0,3800003100,39152941,00.htm.
- **Data Scandal:** According to security experts, a data scandal roll call would include big names in nearly every industry. Some experts say that there are hundreds if not thousands of other, less-publicized cases in which sensitive personal data has been compromised. For CIOs, this trend means two things: It may not be a case of whether your company will experience a data security breach but when it will experience such a breach. And, if you're one of the unlucky 10% or less who find their stories blasted throughout the national news media, you'd better know beforehand how you're going to respond when a breach occurs. Source: http://www.computerworld.com/securitytopics/security/story/0,10801,105065,00.html .
- **Virus attacks fall:** According to two reports, the threat of infection by mass-mailed viruses is decreasing and tailored attacks are on the increase. The number of viruses circulating around the Internet declined in September. Source: http://news.zdnet.co.uk/internet/security/0,39020375,39225761,00.htm.
- **Center allows industry to explore cybersecurity:** The National Science Foundation is sponsoring a new research center to explore short-term solutions to cybersecurity problems. Government, businesses and academic institutions are invited to take part in the Center for Information Protection (CIP), based at Iowa State University. "With over 85 percent of the cyber infrastructure controlled by private industries, it is critical that government, academia and the private sector work together to develop better methods to protect public and private information contained within the infrastructure," said Carl Landwehr, an NSF program director, in a prepared statement. Source: http://www.fcw.com/article90999-10-03-05-Print.
- **Online Crime Rises Dramatically, Report Says:** According to a survey conducted by Symantec, online criminal activity of nearly every variety surged in the first half of 2005, fueled in large part by an increase in software security flaws and in the number of home computers being used against their owners' wishes to distribute spam, spyware and viruses. Symantec also tracked a massive increase in "denial of service" attacks. During this six month period, 1,862 new software vulnerabilities were discovered. Source: http://www.bizreport.com/news/9331/ .
- **Defend your network against idle scanning:** Just blocking the IP address when your organization's intrusion-detection system (IDS) identifies a scan of your network isn't addressing the real threat. Black hats employ several stealth scanning techniques, and one of those threats is the idle

scan. Source: http://insight.zdnet.co.uk/communications/networks/0,39020427,39224417,00.htm.

- **Threat Alert: Spear Phishing:** According to the secretary general of the Anti-Phishing Working Group, spear phishers act much like marketers, crafting a message and then directing it to just the right people. Intercepted spear-phishing attempts exploded from 56 instances in January to more than 600,000 cases in June. Source: http://www.pcworld.com/resource/article/0,aid,122497,pg,1,RSS,RSS,00.asp.
- **Malicious code could trick ZoneAlarm firewall:** Security experts are warning that malicious code that masquerades as a trusted application could trick a ZoneAlarm firewall into letting it connect to the Internet. Source: http://beta.news.com.com/Malicious+code+could+trick+ZoneAlarm+firewall/2100-1002_3-5886488.html?part=rss&tag=5886488&subj=news.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Lovgate.w	Win32 Worm	Slight Increase	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
3	Netsky-D	Win32 Worm	Increase	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
4	Mytob-BE	Win32 Worm	Increase	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
5	Mytob-AS	Win32 Worm	Increase	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
6	Zafi-B	Win32 Worm	Decrease	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
7	Mytob.C	Win32 Worm	Slight Decrease	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
8	Zafi-D	Win32 Worm	Decrease	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
9	Netsky-Q	Win32 Worm	Decrease	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
10	Netsky-Z	Win32 Worm	Slight Decrease	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.

Table updated October 3, 2005

[back to top]